CLAIMS

1. Method of payment by electronic cheque, in particular in the case of a direct transaction between solely:

- a payment issuer furnished with a medium (1) comprising at least one blank electronic cheque certified by a financial institution (BA) and an overall amount useable at least partially in respect of the electronic cheque, and
- a recipient of the payment furnished with a device (3) adapted to receive at least one aforesaid electronic cheque of the abovementioned medium (1),

the method comprising, so that the device (3) can recognize the authenticity of the medium (1) and of a cheque being received,

- a calculation by the medium (1) of a table (5), possibly partial, on the basis of at least one set of k base values (S[1],...S[k]), by applying successively to each of them n times an irreversible function (OWF) with parameter(s) differing preferably with each application and giving k intermediate values n times,
- a calculation by the medium (1) of a secret key (SK) on the basis of the last k intermediate values of order n and, on the basis of this key (SK), a calculation of a distinctive sign (IM_{CF}) of the cheque,
- a transmission by the medium (1) to the device (3) of the distinctive sign (IM_{CF}) calculated for the electronic cheque,
- a financial commitment of the medium (1) in relation to the device (3), as regards the cheque, by supplying to the device (3),
- a first result (O_AC_I) of an irreversible function (OWF) via which was processed the result (AC_I) of a first algorithm (MAC) combining a secret verification key (SVK), originating from the financial institution (BA) issuing the electronic cheque, and dynamic parameters (CDP) of this cheque, and

- a second result (AC_C) of a second algorithm (MAC) combining the secret key (SK) calculated for the medium, the dynamic parameters (CDP) of this cheque and the first result (O_AC_I) hereinabove,

- at least one random/pseudo-random guesstimation, by the device (3), of k numbers m of successive applications of the irreversible function (OWF) to the k base values (S[1],...S[k]), the k numbers m lying between zero and n and possibly being different from one another, the sum of the k numbers m having to be a determined constant,

- a transmission of the result of the guesstimation by the device (3) to the medium (1),

- a response by the medium (1) to the said guesstimation by the device (3), comprising on the one hand, the result (AC_I) of the first algorithm combining the secret verification key (SVK) and the dynamic parameters (CDP) of the cheque and, on the other hand, a set of the k intermediate values obtained during the successive applications of the irreversible function (OWF) to each of the k base values (S[1],...S[k]) the number or numbers of times m lying between zero and n,

- by the device (3):

- successive applications of the irreversible function (OWF) to each of the k intermediate values of order(s) m until the last k intermediate values of order n are obtained,

- a calculation of the said secret key (SK) on the basis of these last k intermediate values of order n and, on the basis of this secret key (SK), a calculation of the distinctive sign (IM_{CF}) of the cheque,

- a comparison of the distinctive sign (IM_{CF}) thus calculated and of the distinctive sign (IM_{CF}) calculated by the medium (1) and received from the latter,

- a verification by calculation and comparison in the device (3) of the said second result (AC_C) of the

second algorithm (MAC) and of that received from the medium (1),

- a verification by calculation and comparison in the device (3) of the said first result (O_AC_I) of an irreversible function (OWF) and of that received from the medium (1) and,

- if the said comparison and verifications each give equality, an acceptance and a storage by the device (3) of the electronic cheque issued by the medium (1).

2. Method according to Claim 1, characterized in that the sum of the k numbers m is a constant equal to n*k/2 if the product n*k is even or, if this product is odd, to (n*k-1)/2.

3. Method according to one or other of Claims 1 and 2, characterized in that it comprises:

- a storage in the medium (1) of at least one electronic cheque template (CF) useable to make at least one aforesaid cheque,

- a transmission by the medium (1) to the device (3) of:

  - a series of h distinctive signs ($IM_{CF}[1...h]$) of a cheque, each associated with a distinct set of k base values (S[1],...S[k]) contained in the medium (1),

  - an index (i), lying between 1 and h, for designating a particular distinctive sign ($IM_{CF}[i]$) from among the h aforementioned distinctive signs,

  - a digital signature ($SIGN_{CF}$) produced by the issuing financial institution (BA) so as to guarantee the said distinctive signs ($IM_{CF}[1...h]$), and

- a use by the device (3), for the said comparison, of the particular distinctive sign ($IM_{CF}[i]$) determined by the index (i) in the guise of distinctive sign (IM_{CF}) received from the medium (1), and

- a verification by the device (3) of the said digital signature ($SIGN_{CF}$) by means of a public key (PK_B) known to the device (3).

4. Method according to any one of Claims 1 to 3, characterized

- in that it comprises, in respect of the transaction, a transmission by the medium (1) to the device (3) of non-secret data which may be the identification (ID_B) of the financial institution (BA) which certifies the electronic cheque and, as appropriate, the public key (PK_B) of the issuing financial institution (BA) and a certificate ($CERT_B$) of this public key (PK_B) issued by a certificate authority (CA), and

- in that the device verifies in this case the authenticity of the said certificate ($CERT_B$) by means of another public key (PK_{CA}), known to the device (3), of the certificate authority (CA).

5. Method according to any one of Claims 1 to 4, characterized in that the medium (1) can be reloaded as regards its overall amount and/or its number (i) of electronic cheques in the course of a link with the abovementioned financial institution (BA) or one of its delegates.

6. Method according to one or other of Claims 1 to 5, characterized in that it comprises, for the calculation of the table (5) by the medium (1), a mother base value (SD_{CF}) common to each column (1...k) of the table (5), and an application to this mother base value of at least one irreversible function (SOWF) preferably with different parameter(s) for each column (1...k).

7. Method according to Claim 5, characterized in that in the course of a reloading of the medium (1), it is furthermore supplied with an identification (ID_{CF}) of cheque templates, updated abovementioned static parameters (SP_{CF}), a series of h distinctive signs ($IM_{CF}[1...h]$), an abovementioned digital signature ($SIGN_{CF}$) and a determined number of base values (S[1],...S[k]) or, as appropriate, of at least one aforesaid common base value (SD_{CF}).

8. Method according to any one of Claims 1 to 7, characterized in that the device (3) records, during a transaction, the result (AC_I) of the first algorithm

and/or, as appropriate, an identification (ID_B) of the aforesaid financial institution (BA) and/or an identification (ID_{CF}) of the template of the electronic cheque received and/or the identification (ID_C) of the medium (1).

9. Method according to any one of Claims 1 to 8, characterized

- in that in respect of incremental payments of the kind by telephone card, the dynamic parameters (CDP) of the cheques moreover comprise:

- the amount or the sequence of amounts corresponding to the authorized incremental payments,

- a base chaining value (Z_0),

- a chaining of successive values (Z_j) which each stem successively from the application of an irreversible function to the immediately following value (Z_{j+1}), and

- in that after having performed with the hereinabove device (3) a protocol for payment by electronic cheque, the medium (1) can perform an incremental payment by supplying the receiving device (3) with successive chaining values (Z_1, Z_2, Z_3,...), the device (3) preserving a record of the last value (Z_j) received and of the corresponding index (j).

10. Method according to any one of Claims 1 to 9, characterized in that it comprises a cancellation of a transaction of payment by cheque from the medium (1) to the device (3).

11. Method according to Claim 10, characterized in that it comprises in respect of the aforementioned cancellation,

- a storage, in the device (3), of at least one electronic cheque template, issued by the financial institution (BB) of the device (3), and of secret data relating to this template,

- a programming of the medium (1) in such a way that the latter cannot receive a payment by cheque other than from the device (3) to which a transaction was previously paid by means of the said medium (1),

the latter storing the cancellation payment cheque until the medium (1) is presented to its corresponding financial institution (BA), in particular for a reloading of the medium (1).

12. Method according to any one of Claims 1 to 11, characterized in that it furthermore comprises steps of inverse authentication via which the medium (1) can for its part recognize the authenticity of the device (3).

13. Method according to Claim 12, characterized in that the steps of inverse authentication are of the same kind as those for the authentication of the medium (1), whilst requiring, as appropriate, only a single distinctive sign (IM_{CF}) of electronic cheque template.

14. Method according to one or other of Claims 12 and 13, characterized in that it comprises, for at least some of the inverse authentication steps, the use of an element (7) for communication between the medium (1) and the device (3), this communication element (7) preferably being held by the payment issuer which holds the said medium (1).

15. Method according to one or other of Claims 1 to 14, characterized in that it comprises, in the medium (1), a combination of each of the various distinctive signs ($IM_{CF}[i]$), at a first level, by means of irreversible functions (OWHF) each time with another value or another distinctive sign ($IM_{CF}[i']$), in that the results (V_1, V_2; V_3, V_4) of each pair of applications of the irreversible function (OWHF) are combined at a second level via another application of the irreversible function (OWHF) so as to give new results (V_5, V_6) to be combined at a third level via one or other applications of the irreversible function (OWHF) and so on and so forth until a single result (O_IM_{CF}) is obtained, and which is signed, as deduced distinctive sign, by the digital signature ($SIGN_{CF}$) so as to sign the cheques issued.

16. Method according to Claim 15, characterized in that it comprises, for a verification by the device (3) of the deduced distinctive sign (O_IM_{CF}), a transmission

from the medium (1) each time of the second distinctive sign ($IM_{CF}[i]$) used in a first combination (OWHF) at the first level and, at each succeeding level, of the intermediate result (V_2, V_6) of the irreversible functions (OWHF), which is used so as to be combined successively with the corresponding intermediate result (V_1, V_5) obtained on the basis of the second distinctive sign ($IM_{CF}[i]$), until the deduced distinctive sign ($O\text{-}IM_{CF}$) is obtained.

17. Payment system for implementing the method according to any one of Claims 1 to 16, characterized in that it comprises

- at least one medium (1) furnished
- with means for storing at least
- a blank electronic cheque certified by a financial institution (BA),
- an overall amount useable at least partially in respect of the electronic cheque,
- at least one distinctive sign (IM_{CF}) for this cheque, which may be included in the latter,
- at least one set of k base values (S[1],...S[k]) which may be derived from a single mother value (SD_{CF}),
- a secret verification key (SVK) originating from the financial institution (BA) issuing the electronic cheque, and
- dynamic parameters (CDP) of the said cheque, and
- with means of calculation
- of a table (5) on the basis of the k base values (S[1],...S[k]), by applying successively to each of them n times an irreversible function (OWF) with parameter(s) differing preferably with each application and giving k intermediate values n times,
- of a secret key (SK) on the basis of the last k intermediate values of order n and, on the basis of this key (SK), of a distinctive sign (IM_{CF}) of the cheque,
- of a first result (O_AC_I) of an irreversible function (OWF) via which was processed the result (AC_I) of a first algorithm (MAC) combining the secret

verification key (SVK) and dynamic parameters (CDP) of the cheque, and

- of a second result (AC_C) of a second algorithm (MAC) combining the secret key (SK) calculated for the medium (1), the dynamic parameters (CDP) of this cheque and the first result (O_AC_I) hereinabove, and

- with means of direct dialogue with at least one device (3) adapted to receive at least one aforesaid electronic cheque from the abovementioned medium (1) and among other things the distinctive sign (IM_{CF}) of the said cheque,

- the device (3) being equipped

- with means of random/pseudo-random guesstimation of k numbers m of successive applications of the irreversible function (OWF) to the k base values (S[1],...S[k]), the k numbers m lying between zero and n and possibly being different from one another, the sum of the k numbers m having to be a determined constant,

- with means of direct dialogue corresponding to those of the medium (1), so as among other things to carry out a transmission of the result of the guesstimation to the medium (1),

- with means of calculation

- successively applying the irreversible function (OWF) to each of the k intermediate values of order m until the last k intermediate values of order n are obtained,

- of the said secret key (SK) on the basis of these last k intermediate values of order n and, on the basis of this secret key (SK), a calculation of the distinctive sign (IM_{CF}) of the cheque,

- means of comparison of the distinctive sign (IM_{CF}) thus calculated and of the distinctive sign (IM_{CF}) calculated by the medium (1) and received from the latter,

- means of verification by calculation and comparison of the said second result (AC_C) of the second algorithm (MAC) and of that received from the medium (1),

- means of verification by calculation and comparison of the said first result (O_AC_I) of an irreversible function (OWF) and of that received from the medium (1) and,

- means of storage of at least the electronic cheque issued by the medium (1), if the said comparison and verifications each give equality.

18. System according to Claim 17, characterized in that:

- the means of storage of the medium (1) are devised so as to store at least one electronic cheque template (CF) useable to make at least one aforesaid cheque,
- the means of dialogue of the medium (1) are devised so as to transmit to the device (3):

- a series of h distinctive signs ($IM_{CF}[1...h]$) of a cheque, each associated with a distinct set of k base values (S[1],...S[k]) contained in the medium (1),

- an index (i), lying between 1 and h, for designating a particular distinctive sign ($IM_{CF}[i]$) from among the h aforementioned distinctive signs,

- a digital signature ($SIGN_{CF}$) produced by the issuing financial institution (BA) so as to guarantee the said distinctive signs ($IM_{CF}[1...h]$), and
- the device (3) is devised so as to use, for the said comparison, the particular distinctive sign ($IM_{CF}[i]$) determined by the index (i) in the guise of distinctive sign (IM_{CF}) received from the medium (1), and
- the device (3) comprises means of calculation devised so as to verify the said digital signature ($SIGN_{CF}$) by means of a public key (PK_B) known to the device (3).

19. System according to Claim 18, characterized in that:

- the means of dialogue of the medium (1) are devised so as to transmit to the device (3) non-secret data which may be the identification (ID_B) of the financial institution (BA) which certifies the electronic cheque and, as appropriate, the public key (PK_B) of the issuing financial institution (BA) and a

certificate ($CERT_B$) of this public key (PK_B) issued by a certificate authority (CA), and

- the device is devised so as to verify the authenticity of the said certificate ($CERT_B$) by means of another public key (PK_{CA}), known to the device (3), of the certificate authority (CA).

20. System according to any one of Claims 17 to 19, characterized in that it comprises as medium (1) a payment card (2) of the integrated circuit type and as device (3) a payment terminal (4) with reading and writing for a card (2) of this type.

21. System according to Claim 20, characterized in that it comprises as medium (1) a payment card (2) of the integrated circuit type and as device (3) a payment terminal (4) with reading and writing for a card (2) of this type and furnished with means of transferring data received from the said card (2), and/or processed by the terminal (4), into storage means (6) detachable from the terminal (4) proper and in particular transportable to a financial institution (BB) so as to perform therein a transfer of the said data.

22. System according to Claim 20, characterized in that, in particular in the case where the device (3) is remote from the issuer of the payment and/or in the case of steps of inverse authentication of the device (3) by the medium (1), the abovementioned medium (1) is composed among other things, on the one hand, of the aforesaid integrated circuit card (2) and, on the other hand, of a communication element (7), for dialogue between the card and the said device (3).